REMARKS

Claims 1-65 remain pending in the application. Reconsideration is respectfully requested in light of the following remarks.

Section 101 Rejection:

The Examiner rejected claims 1-65 under 35 U.S.C. § 101 as being based on non-statutory subject matter. Applicants addressed this rejection in the previous Response. However, the Examiner does not include any remarks regarding Applicants' arguments in the Final Action mailed September 20, 2007. Therefore, Applicants' arguments are repeated below.

Specifically, the Examiner submits that the claimed invention is directed toward nothing more than the abstract idea of a mathematical algorithm. Applicants respectfully traverse this rejection. However, to expedite prosecution, independent claims 1 and 18 were amended in the previous Response. Specifically, claims 1 and 18 were amended to recite a method implemented in a device supporting a cryptography application, and to recite limitations involving the use of a generated result in a cryptography application.

Applicants respectfully remind that Examiner that in *State Street Bank & Trust Co. v. Signature Financial Group, Inc.*, 149 F.3d 1368, 47 USPQ2d 1596 (Fed. Cir. 1998), as discussed in MPEP 2106, the court stated that the relevant claim was statutory because "the transformation of data, representing discrete dollar amounts, by a machine through a series of mathematical calculations into a final share price, constitutes a practical application … because it produces 'a useful, concrete and tangible result' – a final share price". Just like transforming data representing discrete dollar amounts to determine a final share price was considered a practical application and thus statutory in *State Street*, the generation, storage, and use of computation results in a cryptography application is a practical application and thus statutory. Claims 1 and 18 clearly recite a practical application in the technological arts.

Applicants note that claims 43-56 recite a processor comprising an arithmetic circuit for implementing methods similar to those recited in claims 1-42, and are therefore directed toward statutory subject matter. Independent claims 57 and 61 were amended to more clearly indicate that claims 57-63 are directed to a storage medium comprising program instructions executable by a processor supporting a cryptography application that cause the processor to implement methods similar to those recited in claims 1-42. Claims 64 and 65 are directed toward a processor and include means elements, which by statutory definition are structural elements. Also, for reasons similar to those discussed above, Applicants assert that these claims are directed to statutory subject matter.

For at least the reasons above, Applicants respectfully request the removal of the rejection of claims 1-65 under 35 U.S.C. § 101.

Section 102(e) Rejection:

The Examiner rejected claims 1-5, 13-23, 30, 33-46, 49-52 and 56-65 under 35 U.S.C. § 102(e) as being anticipated by Gressel et al. (U.S. Patent 6,748,410) (hereinafter "Gressel"). Applicants respectfully traverse this rejection for at least the following reasons.

Regarding claim 1, contrary to the Examiner's assertion, Gressel fails to disclose all of the limitations of Applicants' claim. Applicants again note that in the Examiner's remarks regarding the rejection of claim 1 (on pages 5-6), he again cites a large number of passages in Gressel as teaching: "feedback of a previous operation into next operation", "arithmetic operation or instructions", "arithmetic structure", "multiplication two values, summing two values utilizing partial (i.e. bit operations, any bit length, high order bits, low order bits) results from previous multiplication", "register usage", "XOR operations" "redundant representation of numbers", "acceleration, improvements of arithmetic operations", "arithmetic operations utilized to generate cryptographic key(s)",

and "processor utilization for key generation", without describing which of these passages (or elements described therein) he believes discloses each of the limitations of claim 1 or how he interprets these passages to teach the specific limitations of claim 1. Applicants again note MPEP 707.07(d), which requires that, in an Examiner's Action, the ground of rejection, should be "fully and clearly stated". **Since the rejection of claim 1 has not been fully and clearly stated, Applicants assert that it is improper.**

Applicants also assert that many of the Examiner's citations do not teach the features suggested by the Examiner. For example, the Examiner cites column 53, lines 13-19 and 49-51 as teaching "feedback of a previous operation into next operation." These passages describe the operation of a linear feedback shift register. **They have absolutely nothing to do with the claimed limitation, *adding implicitly a partial result from a previously executed single arithmetic instruction to generate a result that represents the first number multiplied by the second number summed with the partial result.*** Similarly, the Examiner cites column 2, lines 31-37 as teaching "multiplication two values, summing two values utilizing partial (i.e. bit operations, any bit length, high order bits, low order bits) results from previous multiplication." **This passage does not teach anything about high order bits, low order bits, or utilizing partial results from previous multiplication, as the Examiner has suggested.** Instead, this passage states, in its entirety:

> Further in accordance with a preferred embodiment of the present invention, the employing step includes multiplying a first integer of any bit length by a second integer of any bit length to obtain a first product, multiplying a third integer of any bit length by a fourth integer of any bit length to obtain a second product, and summing the first and second products with a fifth integer of any bit length to obtain a sum.

In other words, this passage describes that pairs of integers of any length may be multiplied together, and then the results may be added together with another integer (the fifth integer) of any bit length. There is nothing in this passage about any of the integers being partial results of a previous instruction, as the Examiner suggests. **Therefore, this passage teaches nothing about implicitly adding a partial result of a previous instruction.** In yet another example, the Examiner cites column 29, lines 43-49 as

teaching "redundant representation of numbers." **This passage actually describes the use of a redundant register. It has absolutely nothing to do with redundant representation of numbers, as the Examiner suggests.** This also has nothing to do with the limitations of claim 1, but appears to be directed to dependent claim 3.

In addition, Applicants assert that the descriptions of individual features listed above do not teach the specific combination of limitations recited in claim 1. For example, a reference in column 3, lines 1-7 to "generate a sum and to feed in the sum to an $(i+1)^{th}$ Montgomery multiplication operation" does not teach the specific limitations regarding implicitly adding a partial result from a previously executed single arithmetic instruction, much less a partial result that comprises a high order portion of a result of the previous instruction. In another example, the Examiner's citations that refer generally to various "arithmetic operation or instructions" or "arithmetic structure" clearly do not teach any of the specific limitations of Applicants' claim.

In the Response to Arguments section of the Final Action mailed September 20, 2007, the Examiner submits that Gressel discloses *adding implicitly a partial result from a previously executed single arithmetic instruction to generate a result that represents the first number multiplied by the second number summed with the partial result*, in column 3, lines 1-7, column 53, lines 13-19 and 49-51, and column 2, lines 31-37. **The Examiner's assertion is not supported by the actual teachings of the reference. As discussed above, these passages clearly do not teach this limitation of claim 1.**

The Examiner then argues, "In very long instruction (VLIW) architectures, which include many microcode architectures, multiple simultaneous operations and operands are specified in a single instruction… This standard computer architecture feature discloses a single arithmetic instruction to perform multiple operations." Applicants assert that no one of ordinary skill in the art would consider a VLIW instruction to be a single arithmetic instruction, as recited in claim 1. Applicants also note that nothing in Gressel describes that it is (or could be) a VLIW architecture. In addition, in a VLIW

architecture, the multiple operations specified by a single instruction are performed simultaneously. Therefore, none of the operations thereof can rely on feedback from others ones of the operations thereof. **Thus, a VLIW instruction does not teach the single arithmetic instruction of Applicants' claim.**

In the Response to Arguments section of the Final Action, the Examiner also submits that Gressel discloses *wherein the partial result comprises a high order portion of a result of the previously executed single arithmetic instruction* in column 2, lines 31-37. The Examiner submits, "The Gressel prior art discloses partial results from an arithmetic operation. The partial results could be the high order bits." **However, as discussed above, this passage does not teach using partial results at all, but instead describes multiplying numbers of any bit length.** Therefore, it cannot and does not teach or suggest that these partial results comprise the high order bits of the result. This clearly does not teach or suggest this limitation of claim 1.

Finally, the Examiner submits that Gressel discloses storing at least a portion of the generated result; and using the stored at least a portion of the generated result in a subsequent computation in the cryptography application in column 3, lines 1-7, and column 53, lines 13-19 and 49-51, "feedback of a previous operation into a next (subsequent operation)." As discussed above, these passages do not teach the feedback feature recited in claim 1. In addition, they teach nothing about using at least a portion of the generated result (i.e., the result of the operations recited in claim 1) in a subsequent computation in a cryptography application or in any other application.

Applicants again remind the Examiner that anticipation requires the presence in a single prior art reference disclosure of each and every limitation of the claimed invention, **arranged as in the claim**. M.P.E.P 2131; *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984). The **identical invention must** be shown in as complete detail as is contained in the claims. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). As discussed above, Gressel clearly does not disclose all of the specific limitations of claim 1.

For at least the reasons above, Gressel cannot be said to anticipate claim 1 and removal of the rejection there is respectfully requested.

Claims 43, 57, and 64 include limitations similar to those recited in claim 1 and discussed above, and were rejected for the same reasons as claim 1. Therefore, the arguments presented above apply with equal force to these claims, as well.

Regarding claim 18, contrary to the Examiner's assertion, Gressel fails to disclose all the limitations of this claim. Claim 18 includes limitations similar to those recited in claim 1 and discussed above, and was rejected for the same reasons as claim 1. Therefore, Applicants traverse this rejection for at least the reasons presented above regarding limitations in this claims that are similar to those in claim 1. In addition, claim 18 recites *adding a third number to generate a result that represents the first number multiplied by the second number summed with the partial result and the third number.* The Examiner does not include any additional remarks regarding this limitation or any additional citations in the reference to teach it. **Applicants assert that the Examiner's citations regarding feedback from previous operations and the multiplication and/or addition of integers of any bit length teach nothing about a single arithmetic instruction that results in the operations recited in claim 1 with or without the additional limitation recited in claim 18.**

For at least the reasons above, Gressel cannot be said to anticipate claim 18 and removal of the rejection there is respectfully requested.

Claims 50, 61, and 65 include limitations similar to those recited in claim 18 and discussed above, and were rejected for the same reasons as claim 18. Therefore, the arguments presented above apply with equal force to these claims, as well.

Regarding claim 2, contrary to the Examiner's assertion, Gressel fails to disclose *performing the adding of the partial result as part of addition operations performed for*

the multiplying of the first and second number. The Examiner again cites column 2, lines 31-37 as teaching this limitation. **However, as discussed above, this passage teaches nothing about adding a partial result of an operation at all, much less adding the partial result as part of addition operations performed for multiplying the first and second number, as recited in claim 2.**

For at least the reasons above, Gressel cannot be said to anticipate claim 2 and removal of the rejection there is respectfully requested.

Claim 19 includes limitations similar to those recited in claim 2 and discussed above, and was rejected for the same reasons as claim 2. Therefore, the arguments presented above apply with equal force to this claim, as well.

Regarding claim 3, contrary to the Examiner's assertion, Gressel fails to disclose *wherein the partial result is in redundant number representation*. The Examiner again cites column 29, lines 43-49 as teaching this limitation. **However, as discussed above, this passage describes a redundant register. It has absolutely nothing to do with a partial result being in redundant number representation.**

For at least the reasons above, Gressel cannot be said to anticipate claim 3 and removal of the rejection there is respectfully requested.

Claims 20, 45, and 52 include limitations similar to those recited in claim 3. Therefore, the arguments presented above apply with equal force to these claims, as well.

Regarding claim 4, contrary to the Examiner's assertion, Gressel fails to disclose *wherein said adding the partial result comprises adding the partial result to a multiplication result of the first and second numbers*. The Examiner again cites column 2, lines 31-37 as teaching this limitation. **However, as discussed above, this passage teaches nothing about adding a partial result of an operation at all, much less**

adding the partial result to a multiplication result of the first and second numbers, as recited in claim 4.

For at least the reasons above, Gressel cannot be said to anticipate claim 4 and removal of the rejection there is respectfully requested.

Regarding claim 5, contrary to the Examiner's assertion, Gressel fails to disclose *wherein said storing at least a portion of the generated result comprises storing a high order portion of the generated result as a next partial result for use with execution of a subsequent single arithmetic instruction*. The Examiner again cites column 3, lines 1-7, and column 53, lines 13-19 and 49-51, "feedback of a previous operation into a next operation". **However, as discussed above, these passage teach nothing about storing a portion of a result for use in a subsequent instruction, much less the specific limitations recited in claim 5.**

For at least the reasons above, Gressel cannot be said to anticipate claim 5 and removal of the rejection there is respectfully requested.

Claims 23 and 51 include limitations similar to those recited in claim 5. Therefore, the arguments presented above apply with equal force to these claims, as well.

Regarding claim 13, contrary to the Examiner's assertion, Gressel fails to disclose *the single arithmetic instruction is a single multiply-accumulate instruction; wherein the first and second numbers are specified in the single multiply-accumulate instruction as first and second source registers, and a low order portion of the result is stored in a destination location specified in the single multiply-accumulate instruction.* The Examiner again cites column 3, lines 1-7, and column 53, lines 13-19 and 49-51, "feedback of a previous operation into a next operation", along with col. 3, lines 28-32, and column 11, lines 7-11 and 40-49 "arithmetic operation or instructions" as teaching these limitations. **However, as discussed above, the Examiner's citations regarding feedback do not teach the use of a partial result in a subsequent operation, as in**

Applicants' claims. In addition, the general references to arithmetic operations or instructions in columns 3 and 11 teach nothing about the specific limitations recited in claim 13.

For at least the reasons above, Gressel cannot be said to anticipate claim 13 and removal of the rejection there is respectfully requested.

Regarding claim 14, contrary to the Examiner's assertion, Gressel fails to disclose *wherein the first and second numbers are n-bit numbers, n being a positive integer, and wherein the high order portion of the generated result is an n-bit portion*. The Examiner again cites column 2, lines 31-37. **However, as discussed above, this passage teaches nothing about a partial result comprising a high order portion of a generated result, much less one having a same number of bits as the recited first and second numbers.**

For at least the reasons above, Gressel cannot be said to anticipate claim 14 and removal of the rejection there is respectfully requested.

Regarding claim 15, contrary to the Examiner's assertion, Gressel fails to disclose *in response to executing the subsequent single arithmetic instruction, multiplying third and fourth numbers specified by the subsequent single arithmetic instruction and adding implicitly the next partial result to generate a second result that represents the third number multiplied by the fourth number summed with the next partial result*. The Examiner again cites column 2, lines 31-37, along with col. 3, lines 28-32, and column 11, lines 7-11 and 40-49 "arithmetic operation or instructions" as teaching these limitations. **However, these citations teach nothing about a <u>subsequent single arithmetic instruction</u> (i.e., one in which a partial result of the earlier recited single arithmetic instruction is used) much less that the specific operations recited in claim 15 are performed in response to such an instruction.**

For at least the reasons above, Gressel cannot be said to anticipate claim 15 and removal of the rejection there is respectfully requested.

Claim 59 includes limitations similar to those recited in claim 15. Therefore, the arguments presented above apply with equal force to this claim, as well.

Regarding claim 16, contrary to the Examiner's assertion, Gressel fails to disclose *storing the high order portion of the second result to be implicitly added in response to executing another subsequent single arithmetic instruction*. The Examiner again cites column 3, lines 1-7, and column 53, lines 13-19 and 49-51, "feedback of a previous operation into a next operation", along with column 2, lines 31-37. However, these passages teach nothing about a second result of a subsequent single arithmetic instruction, and therefore, nothing about storing the high order portion of such a second result to be added to yet another subsequent single arithmetic instruction, as recited in claim 16.

For at least the reasons above, Gressel cannot be said to anticipate claim 16 and removal of the rejection there is respectfully requested.

Claim 38 includes limitations similar to those recited in claim 16. Therefore, the arguments presented above apply with equal force to this claim, as well.

Regarding claim 17, contrary to the Examiner's assertion, Gressel fails to disclose *wherein the multiplying and adding are implemented to support XOR operations for binary polynomial fields*. The Examiner cites column 8, lines 59-60 and column 53, lines 13-19, "XOR operations" as teaching this limitation. These passages describe XOR circuitry in the system of Gressel that is used during a multiplication operation and in a Johnson counter. **They have absolutely nothing to do with XOR operations (or any other operations) for binary polynomial fields, or the multiplying and adding of Applicants' claims being implemented to support such operations.**

For at least the reasons above, Gressel cannot be said to anticipate claim 17 and removal of the rejection there is respectfully requested.

Claim 42 includes limitations similar to those recited in claim 17. Therefore, the arguments presented above apply with equal force to this claim, as well.

Regarding claim 36, contrary to the Examiner's assertion, Gressel fails to disclose *in response to executing the subsequent single arithmetic instruction, multiplying a fourth number and a fifth number, the fourth number being specified by the subsequent single arithmetic instruction, adding implicitly the next partial multiplication result, and adding a sixth number to generate a second result, the second result representing the fourth number multiplied by the fifth number summed with the next partial result and the sixth number*. The Examiner again cites col. 3, lines 28-32, and column 11, lines 7-11 and 40-49 "arithmetic operation or instructions" as teaching these limitations. **Again, Applicants assert that the generic references to arithmetic operations or instructions in these passages teach absolutely nothing about the specific limitations recited in claim 36.**

For at least the reasons above, Gressel cannot be said to anticipate claim 36 and removal of the rejection there is respectfully requested.

Claims 60, 62, and 63 include additional limitations reciting additional multiplication and implicit addition operations that are performed in response to subsequent single arithmetic instructions. **Applicants assert that nothing in the Examiner's citations, or elsewhere in Gressel, discloses these subsequent single arithmetic operations and corresponding multiplication and implicit addition operations.**

Regarding claim 37, contrary to the Examiner's assertion, Gressel fails to disclose *wherein the fifth number and the second number are equal*. The Examiner again cites column 29, lines 43-49 "representation of numbers". **However, as discussed above, this passage has nothing to do with "representation of numbers." Instead, it describes "four main serial main registers," one of which is redundant.**

For at least the reasons above, Gressel cannot be said to anticipate claim 37 and removal of the rejection there is respectfully requested.

Regarding claims 30, 33, 34, 35, 39, 40, 41, 49, 56, and 58, contrary to the Examiner's assertion, Gressel fails to disclose the limitations recited in these claims. Theses claims recite limitations involving the implicit and explicit identification by the single arithmetic instruction and in subsequent single arithmetic instructions of the various operands that are multiplied and added in Applicants' claimed invention. **Applicants assert that none of the Examiner's citations, or anything else in Gressel, discloses the specific limitations recited in these claims regarding the identification of these operands in single arithmetic instructions.**

Section 103(a) Rejection:

The Examiner rejected claims 6-12, 24-29, 31, 32, 47, 48, 53, 54 and 55 under 35 U.S.C. § 103(a) as being unpatentable over Gressel in view of Stribaek et al. (U.S. Patent 7,181,484) (hereinafter "Stribaek"). Applicants respectfully traverse this rejection for at least the following reasons.

Regarding claim 6, contrary to the Examiner's assertion, Gressel in view of Stribaek fails to teach or suggest *wherein said storing the high order portion of the generated result comprises storing the high order portion of the generated result into an extended carry register for use with execution of the subsequent single arithmetic instruction*. The Examiner submits that Gressel teaches storing the high order portion of the generated result for use with execution of the subsequent single arithmetic instruction. **However, as discussed above, Gressel does not teach this limitation.**

The Examiner admits that Gressel does not specifically disclose an extended carry register and relies on Stribaek to teach this feature in column 5, lines 41-45. The Examiner submits that it would have been obvious to one of ordinary skill in the art to

modify Gressel as taught by Stribaek to enable the capability for the usage of an extended carry register to enable the capability for extended precision arithmetic calculations due to extensive and increasing usage of public key cryptography. While Stribaek does describe an extended carry register and its usefulness in extended precision arithmetic, it does not teach or suggest the specific use of such a register recited in claim 6. In fact, the Examiner citation states, "Similarly, the instruction format for MTLHX ("Move to Lo, Hi and Extended Carry") is shown in FIG. 10B. When executed, an appropriate number of bits (e.g., eight) of the value in HI register 2022 are written into the ACX register 2021." This describes that a specific move-type instruction is used for loading the extended carry register. **This clearly does not teach that a partial result is (or could be) stored in an extended carry register in response to the single arithmetic instruction that also performs the addition and multiplication operations recited in claim 1.** Therefore, adding this extended carry register and its special load operation to the system of Gressel clearly would not result in the claimed invention.

Applicants remind the Examiner that to establish a *prima facie* obviousness of a claimed invention, all claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974), MPEP 2143.03. Applicants assert that, as discussed above, the cited references do not teach the limitations of claim 6, whether taken alone or in combination.

For at least the reasons above, the rejection of claim 6 is unsupported by the cited art and removal thereof is respectfully requested.

Claims 7, 8, 10, 24-27, and 44 also recite limitations involving an extended carry register into which partial results are loaded and/or from which they are retrieved in response to a single arithmetic instruction. Therefore, the arguments presented above apply with equal force to these claims as well.

In regard to the rejections under both § 102(e) and § 103(a), Applicants also assert that numerous other ones of the dependent claims recite further distinctions over the cited art. Applicants traverse the rejection of these claims for at least the reasons given above in regard to the claims from which they depend. However, since the rejections have been shown to be unsupported for the independent claims, a further discussion of the dependent claims is not necessary at this time. Applicants reserve the right to present additional arguments.

CONCLUSION

Applicants submit the application is in condition for allowance, and notice to that effect is respectfully requested.

If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/6000-32301/RCK.

Respectfully submitted,

/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicants

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: November 20, 2007